IN THE U.S. DISTRICT COURT FOR MARYLAND,
SOUTHERN DIVISION

BEYOND SYSTEMS, INC.	*	
	*	
Plaintiff	*	
	*	
v.	*	**Case No. PJM 08 cv 0921**
	*	
WORLD AVENUE USA, LLC, ET AL.	*	
	*	
Defendants	*	

PLAINTIFF'S MOTION TO COMPEL NON-PARTY DNSMADEEASY.COM, LLC TO RESPOND FULLY TO SUBPOENA FOR DOCUMENT PRODUCTION, AND FOR CONTEMPT, AND FOR SANCTIONS

Plaintiff served non-party DNSMadeEasy.com, LLC, dba "Tiggee," with a subpoena for production of documents only. Tiggee has failed to make any production. Defendant World Avnue USA, LLC has filed an untimely motion for protective order seeking to prevent Tiggee from producing the documents sought in the subpoena.

I. Background.

Plaintiff, Beyond Systems, Inc. (BSI), sued Defendants for initiating, or conspiring in the initiation of, commercial email containing certain false or deceptive information in violation of Maryland and Florida anti-spam statutes. Amended Complaint at d. 134. Defendants are part of a group of entities owned or controlled by Defendant Niuniu Ji and his family, sharing offices and other resources in what appears to be a common enterprise. Defendants, who refer to themselves variously as the "World Avenue companies," or as World Avenue and its "sister companies," routinely create new entities, and conduct mergers, acquisitions and name changes for those entities that obscure their roles and identities. Plaintiffs contend that all of the World

Avenue companies work in concert as part of a single enterprise, and are co-conspirators in the wrongs alleged in this suit.

Defendants are in the "lead generation" business, which is to say that they gather names and contact information from recipients of their advertisements, and create lists that are then sold to other marketers. In order to gather the contact information Defendants enlist "affiliates" who in turn use "creatives" or advertising content provided by Defendants in emails that are transmitted to millions of email addresses. These emails "drive traffic," or induce recipients to click on links that take them to websites, which in turn induce the recipients to enter their names and contact information, sometimes in return for "free gifts." The affiliates are paid by Defendants based on the outcome of the email campaigns, measured in various ways. Defendants are fully aware that email is the primary means used by the affiliates to promote Defendants' business.

In order to evade liability Defendants avoid having their names placed in the emails. In order to minimize liability for the affiliates, Defendants assist them in remaining anonymous. In furtherance of the emphasis on anonymity, Defendants use hundreds of domain names and trade names in connection with websites through which the "lead generation" takes place. Most, if not all, of the domain names so used are registered to fictitious or false names, rendering the domain name registration of no use for purposes of identifying the real identities of the persons behind the emails or the marketing schemes which rely on them.

Plaintiff initially filed a motion for expedited discovery, which was denied. Only limited discovery has been obtained to this point, due in part to delays from Defendants' motions to dismiss, and now due to intransigence from defendant at every turn. See BSI's motion to compel regarding jurisdictional discovery at docket 138 and motion to quash subpoenas to non-parties at docket 157.

II. The Subpoena to Tiggee

BSI served Tiggee with the subpoena on January 2, 2010 by certified mail. Copies of the subpoena and certified mail receipt are attached as Exhibits 1 and 2, respectively. Tiggee responded through its president, Steven Job, acknowledging receipt of the subpoena. A copy of Mr. Job's statement of January 10, 2010, promising a "report," is attached as Exhibit 3. Mr. Job promised,

> Tiggee will provide a detailed report of all information regarding the DNS services for the domains in the "WorldAvenue" account within DNS Made Easy. To the best of my knowledge, this will provide all of the information available to us according our data records. Generating and delivering a report of this nature will take a significant amount of time and resources that Tiggee will expect to be reimbursed by Beyond Systems / Steven H. Ring PC.

Exhibit 3. Tiggee further responded through counsel in a series of emails that started out in cooperative fashion, but then took a sudden turn downward. Before going south, those emails included additional promises of cooperation and production of responsive documents as follows:

Email Jan 21, 2010 from Mr. Etelson to Mr. Ring:

> So to confirm our conversation, we have agreed for now that we will produce, in
> response to the
> subpoena:
> 1. A sampling of 15 domain names from the list on your subpoena with associated
> DNS
> information (IP addresses)
> 2. We will produce the account information for World Ave, LLC that Tiggee has
> 3. We will produce name of the payor on the account, the address for the payor,
> along with the
> dates and amounts of payment. We also confirm payments were made by credit
> card, but will
> not produce the credit card number without a court order.

Email January 25, 2010 from Mr. Etelson to Mr. Ring:

> Steve,
> I received your voicemail. While we are working on providing the information, which we are hoping to provide by the end of this week, as I told you, I cannot produce anything until you advise me of what counsel for the defendants received. Please advise whether they were sent a copy of the subpoena with the attachment and we it was sent to them.

Exhibit 7, attached. After January 25, 2010 Tiggee grew increasingly evasive. On February 5, 2010, a motion for protective order was filed, not by DNS, but by Defendant World Avenue. USA, LLC (WAUSA). Tiggee has made no production as of this writing.

The subpoena lists definitions, and seeks production of the following:

1. All DOCUMENTs RELATED to any of the following domain names:

[list of approximately 150 names linked to World Avenue, beginning with SuperbRewards.com, travel-ncs.com 123SpecialGifts.com, AmericanSurveyPanel.com, AmericasTopBrands.com, etc.]

2. All DOCUMENTs RELATED to the registration of the domain names listed above.

3. All DOCUMENTs RELATED to the purchase, lease or use of the domain names listed above.

4. All DOCUMENTs RELATED to the sale, resale, exchange or ownership of the domain names listed above.

5. All DOCUMENTs RELATED to hosting or provision of DNS service or any other service for the domain names listed above.

6. All DOCUMENTs RELATED to or complaints related to the domain names listed above.

7. All DOCUMENTs RELATED to the identification of, or communications with, any person who registered, purchased, leased, sold, resold, owned or used any of the domain names listed above, or received or paid for any service related to those domain names.

8. All DOCUMENTs RELATED to any person besides YOU who registered, purchased, leased, sold, resold, owned or used any of, or received any service for, the domain names listed in the previous document request, including any records of domain name registrations.

9. All DOCUMENTs RELATED to WORLD AVENUE not produced in the previous requests, including any records of any other domain name registrations.

10. All DOCUMENTs RELATED to WORLD AVENUE.

The subpoena was reasonably tailored to these 10 subject areas to minimize the inconvenience to Tiggee. The information sought from DNSMadeEasy.com, LLC is an important part of connecting the emails that give rise to this case with Defendants, due in large part to the deception used in the marketing scheme to obscure the path of responsibility.

III. The Need for Domain Name and DNS Information

Defendants conduct their online marketing business, which is based largely on bulk email, using dozens of corporate names, domain names, trade names, fictitious names, URL’s and websites. A multitude of names is needed to help conceal the nexus between the affiliates who most directly send the emails, and the World Avenue companies who benefit from those emails. The World Avenue companies take great pains to obscure any publicly viewable connections with their affiliates, despite their central role in sending the emails.

Public records on file in this case address the following entities in the World Avenue family of companies spawned by Defendant Niuniu Ji:1) World Avenue USA, LLC t/a "TheUseful," 2) The Useful, LLC, announcing itself as “a World Avenue Company” on its website as shown at docket 34-13, 3) World Avenue Holdings, LLC, 4) Niupercent, Inc., 5) Net Radiance, LLC, 6) World Avenue Management, Inc., 7) World Avenue IP, LLC, 8) World Avenue, LLC, 9) Apercent, LLC 10) World Avenue (Bermuda) Limited Corp., 11) Infrastructure International Limited Corp. 12) LAD Express and 13) World Avenue Services, LLC. Mr. Ji has in recent years set up operations in the Virgin Islands and Bermuda, adding a host of other entities. Public records repeatedly list the following individuals in various positions with the U.S., Virgin Islands and Bermuda-based companies: 1) Niuniu Ji, 2) Yuandong Ji, 3) Dale Baker, 4) Allison Smith and 5) Michael Bryant.

Simple domain name lookups for the domain names that appear in the emails that give rise to this suit lead to phony names, or to "privacy services" which refuse to divulge the real names of the registrants. Tiggee provides DNS or domain name service, which maps IP addresses to domain names. This service is necessary for the functionality of the domain names. DNS mapping is more likely to lead to the true identity of the owner of the domain name. See Affidavit of Paul A. Wagner, attached.

Without tapping DNS data, an outsider does not have the ability to ascertain all of the domain names owned or used by the World Avenue companies. BSI does not have the ability to ascertain

<u>IV. Internet Terminology</u>

In the case of <u>In re Pharmatrak, Inc. Privacy Litigation</u>, 329 F.3d 9 (1st Cir. 2003) the court set forth some useful definitions in footnotes as follows:

> 1. An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215
>
> 2. URLs (Uniform Resource Locators) are unique addresses indicating the location of specific documents on the Web. The webpage a user viewed

> immediately prior to visiting a particular website is known as the referrer URL. Search engines such as Yahoo! are common referrer URLs
>
> 3 HTML is a coding language used to create documents for the Web. M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary>
>
> 4 M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary> (defining and discussing cookies). A browser, in turn, is a user's interface to the Web
> . . .
> 8 The most popular domain extensions are .com (used by for-profit entities), .edu (academic entities), .gov (government), and .org (not-for-profit)

329 F.3d at 18. Further background on terminology that arises in this case is found in Thomas v. Network Solutions Inc. 176 F3d 500 (CA DC 1999), as follows:

> This is an appeal from the judgment of the district court dismissing a complaint filed against the National Science Foundation ("NSF") and its private contractor, Network Solutions, Inc. Plaintiffs are individuals and entities who registered Internet domain names through Network Solutions, Inc., paying a one-time registration fee and yearly renewal fees thereafter, a portion of which the company paid over to NSF according to the terms of a government contract. The complaint alleged, among other things, that NSF had imposed and collected an unconstitutional tax, that Network Solutions had violated the antitrust laws, and that the amount of the fees charged pursuant to the contract exceeded a limitation imposed by statute.
>
> The Internet, "an international network of interconnected computers," Reno v. ACLU, 521 U.S. 844, 117 S.Ct. 2329, 2334, 138 L.Ed.2d 874 (1997), developed from the ARPANET, a network the United States military created in 1969 to link its computers with those of defense contractors and universities. See 63 Fed.Reg. 31,741 (1998). The ARPANET, which no longer exists, served as a model for similar nonmilitary networks. See id.; see also 63 Fed.Reg. 8826 (1998). These networks eventually linked with each other and coalesced into the backbone of the modern Internet, see 63 Fed.Reg. at 8826, enabling tens of millions of people to communicate with one another and to gain access to vast amounts of information from around the world, see ACLU, 117 S.Ct. at 2334.
>
> Internet use has grown dramatically in the past two decades. The number of networked "host" computers--those that store information and relay communications--increased from about 300 in 1981 to approximately 9.4 million in 1996. See id. Roughly 60 percent of these host computers are located in the

United States. See id. About 40 million people used the Internet in 1996, a number expected to rise to 200 million this year. See id.

Individuals generally obtain access to the Internet through these host computers, each of which has a numerical address, or Internet Protocol number, such as "98.37.241.30," that allows other host computers to identify and locate it.1 See 63 Fed.Reg. at 8826; see also 63 Fed.Reg. at 31,741. When the Internet was in its infancy, Internet Protocol numbers were assigned and maintained by the late Dr. Jon Postel, then a UCLA graduate student working under a contract between the Defense Department and the university. See 63 Fed.Reg. at 31,741. When Dr. Postel moved from UCLA to the Information Sciences Institute at the University of Southern California, he continued to maintain the lists pursuant to contracts with the Defense Department. See id. As the lists grew, Dr. Postel delegated certain aspects of the list maintenance to what eventually became known as the Internet Assigned Numbers Authority. See id.

Because many numerical sequences are difficult to remember, the Internet community created a system allowing an Internet computer to be identified by a "domain name." See 62 Fed.Reg. 35,896 (1997). The domain name system is a hierarchy. See 63 Fed.Reg. at 8826. Top-level domains are divided into second-level domains, and so on. See id. More than 200 national, or country-code, top-level domains--e.g., ".us" for the United States, ".pa" for Panama, ".uk" for the United Kingdom, and so on--are administered by their corresponding governments or by private entities with the government's permission. See 63 Fed.Reg. at 31,742. A small set of generic top-level domains carry no national identifier, but denote the intended function of that portion of the domain space: ".com" for commercial users; ".org" for non-profit organizations; ".net" for network service providers; ".edu" for educational institutions; ".gov" for United States government institutions; ".mil" for United States military institutions; and ".int" for international institutions. See 63 Fed.Reg. at 31,742.

Domain names--e.g., bettyandnicks.com--consist of at least two groups of alphanumeric characters, each known as a string, separated by a period or dot. The last string--the farthest to the right--denotes the top-level domain. The second-to-last string is the second-level domain name and identifies the person's or organization's Internet computer site. See Albert, supra note 1, at 783. Each string may contain up to 63 characters but the overall domain name must be less than 256 characters. See PGMedia, Inc., No. 97 Civ. 1946 RPP, slip op. at 3.

For the domain name system to function, each domain name must be unique and correspond to a unique Internet Protocol number. See 63 Fed.Reg. at 8826; see also Goldfoot, supra note 1, at 913. A new user who wishes to have an Internet site with a domain name address first obtains an Internet Protocol number (e.g., 1.23.456.7). See PGMedia, Inc., No. 97 Civ. 1946 RPP, slip op. at 5. The

> user then registers a domain name and it becomes linked with that Internet Protocol number. See id. at 5-6.
>
> **Before using a domain name to locate an Internet computer site in "cyberspace," a computer must match the domain name to the domain name's Internet Protocol number.2 The match information is stored on various Internet-connected computers around the world known as domain name servers**. The computer attempts to find the match information by sending out an address query.3 The goal of the address query is to find the particular domain name server containing the match information the user seeks. See id. at 4-5.
>
> When ordered to translate an unknown domain name into an Internet Protocol number, a computer will ask its Internet Service Provider's server if it knows the domain name and corresponding Internet Protocol number. See Albert, supra note 1, at 785. If that server lacks the information, it will pass the query to a "root server," also called a "root zone" file, the authoritative and highest level of the domain name system database.4 See 63 Fed.Reg. at 8826. The root zone file directs the query to the proper top-level domain zone file, which contains the domain names in a given domain and their corresponding Internet Protocol numbers. See 63 Fed.Reg. at 8828. In the case of someone searching for the "bettyandnicks.com" home page, the root zone file sends the query to the top-level domain zone file with information about ".com" domain names. The ".com" zone file then refers the query to a second-level domain name file with all the second-level domain names under ".com." This is where the "bettyandnicks.com" query ends: the second-level domain name file has the information matching the domain name to its associated Internet Protocol number. With the Internet Protocol number, the user's computer can connect the user to the requested Internet site. The "bettyandnicks.com" home page will appear, just as if the user had typed in the Internet Protocol number instead of the domain name. See PGMedia, Inc., No. 97 Civ. 1946 RPP, slip op. at 5.

176 F3d at 503-505. [Emphasis added.]

An analogy frequently used to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.example.com translates to 208.77.188.166. http://en.wikipedia.org/wiki/Domain_Name_System What Tiggee provides is the service that essentially offers to the public those “public” entries for the Defendants for the entire Internet to see. Plaintiff seeks from Tiggee information which is available and given out to anyone and everyone on the Internet without limitation IF the requestor knows what to ask. The reason this information has to be request by subpoena from Tiggee is at least two-fold, 1) there are 192 Million Domain Name Registrations (www.verisign.com/domainbrief) and so Tiggee must identify which of these names relate to the Defendants; and 2) Tiggee has set its servers to deny the efficient Tiggee zone transfer of the domains they host, necessitating a unique request for each record type of each domain and subdomain. Defendants cannot claim as confidential records whose contents are publicly viewable, if only one knew which tree in the vast forest for which to ask.

The process of seeking one record at a time for each domain name, without knowing the entire set of domain names owned or used by World Avenue, is endless. Tiggee <u>does</u> know which of World Avenue's domains it services, and is in a position, using simple search techniques, to provide the requested DNS mapping information. We expect this data would be presented in a simple spreadsheet that includes one column for domain names and one column for matching IP addresses, in addition to other information about each such match, such as contact information for a particular World Avenue entity.

V. Tiggee's Objections

The Terms and Conditions of Tiggee clearly state that Tiggee may divulge personal identification information in response to a subpoena. Exhibit 5. The Acceptable Use Policy of Tiggee contains a statement against facilitating spam and concealment of responses to spam. Exhibit 6. By concealing the information sought here, Tiggee is acting against its own policy by protecting the identities of persons engaged in the use of unsolicited commercial email in violation of applicable law. No compelling argument based on privacy has been presented. A protective order has been put in place, largely at Defendants' insistence and with Plaintiff's assent, to address just this type of scenario. There is no basis for the withholding of documents.

Attached to the subpoena is a list of some 150 domain and trade names that appear in some of the emails that give rise to this suit. These names can be considered as partial "fingerprints" that can be used to help track down their owners, but the prints are imperfect and the databases against which they can be matched are not generally available, except for one-by-one match-ups if one knows which name to look for. The size of the list simply reflects the practices of the senders of the emails: they use a rotation of domain and trade names in their marketing efforts. Tiggee has not specified any particular burden involved in providing the information sought in the subpoena. Retrieval and production of that information should be a trivial task, involving simple search commands, and the data can be saved to disc or sent as an email attachment, to minimize the inconvenience to DNS. Plaintiff is no longer seeking mere samples, and now seeks the full scope of the information described in the subpoena.

Tiggee has failed to state any grounds that would justify its failure to comply with the subpoena under applicable law. It has failed to state anything close to an argument for undue burden: it has spent more on counsel fees than its unfounded demand for costs in the January 10, 2010 pro se response, and will likely incur much more than that as a result of its refusal to honor its obligations under the subpoena. It is obvious that Tiggee is ripe for a live deposition, in which event it would not be entitled to costs beyond a modest witness fee.

Tiggee is in a business in which it should expect an occasional subpoena, as a repository of information on Internet marketers. With the multitude of laws now enacted to protect various rights involving the Internet, a DNS service provider should expect to receive a document subpoena in the routine course of business. By the ready response initially, it is apparent that the search required to obtain the data was not in fact burdensome, as Tiggie stood ready to produce at least some of it until World Avenue interfered.

In a recent case involving enforcement of a subpoena to a non-party for production of documents, Magistrate Judge Grimm stated as follows:

> Although a non-party in this case, Synergy is subject [**9] to the same obligations and scope of discovery under Rule 45 as if it were a party proceeding under Rule 34. FED. R. CIV. P. 45, Comm. Notes, 1991 Amend. Sub (a). Under Rule 34, failure to make particularized objections to document requests constitutes a waiver of those objections. Marens v. Carrabba's Italian Grill, 196 F.R.D. 35 (D. Md. 2000); [*329] Thompson v. HUD, 199 F.R.D. 168 (D.Md. 2001); Hall v. Sullivan, 231 F.R.D. 468 (D.Md. 2005). Unfortunately, Synergy did not particularize its objections to these requests, and instead used the boilerplate objections that this Court repeatedly has warned against, thereby waiving its objections.
>
> Although this is the case, Ms. Anderson's request for "all documents concerning the operation of the Nottingham net branch of Synergy Mortgage Corp." (Judg. Cred. Reply at 15) is so overbroad on its face that whole-sale waiver would be unfair. Instead, I will order Synergy to produce for Ms. Anderson's review all non-privileged documents in its possession, custody or control relating to whether Synergy is a successor in interest to Access One. Further, the parties [**10] will be ordered to negotiate a confidentiality agreement regarding any potentially confidential customer information disclosed during this process. Ms. Anderson and Synergy are to negotiate this agreement within fifteen (15) days of the entry of the accompanying order, and Synergy will be ordered to produce the documents requested within thirty (30) days thereafter.

Sabol V. Glenn Brooks, 469 F. Supp. 2d 324; 2006 U.S. Dist. LEXIS 94545. Here, as in Sabol, Tiggee is "subject to the same obligations and scope of discovery under Rule 45 as if it were a party . . ." and its "failure to make particularized objetions to document requests constitutes a waiver of those objections." Its pro-se objections are therefore waived. The later-filed motion for protective order filed by Defendant WAUSA, which is addressed in a separate opposition, does not save Tiggee. Regardless of either filing, the objections to the subpoena fail on their merits. The subpoena is reasonably tailored to the subject matter at issue, and neither Tiggee nor WAUSA has demonstrated any burden that would justify Tiggee's failure to produce.

The subject of the claims in this suit is an ongoing stream of emails from 2004 to the present. Any attempt to confine discovery to a shorter time period is misplaced. Plaintiff alleges in the Amended Complaint: at docket 34:

> 61. Between July 20, 2004 and September 3, 2005, Plaintiff received on its computer servers in Maryland over 68,000 commercial electronic mail messages promoting products or services offered by World Avenue and its agents. Since July 3, 2005 Plaintiff has received thousands of additional emails from WORLD AVENUE.
>
> 62. As used herein, the term, "EMAILS AT ISSUE" means the unsolicited commercial emails that Plaintiff received from WORLD AVENUE, including all emails received up to the date of the entry of any final, non-appealable judgment.
>
> . . .
>
> 68. Defendant JI directed, participated in, stood to derive revenue, and actually derived revenue, as a result of the transmission of the EMAILS AT ISSUE. JI communicated with the managing agents and employees of WORLD AVENUE, and those entities under contract to him, on each of the dates of transmission of the EMAILS AT ISSUE, beginning on or before July 20, 2004 and continuing up to the present, in furtherance of the campaigns to transmit those emails.

Amended Complaint at docket 34. [Emphasis added.] WAUSA has consistently argued, and now attempts to persuade Tiggee, that the relevant time period for discovery ended years ago. Tiggee indicates that it began its services for the World Avenue companies during June of 2009. Plaintiff has received emails containing links that lead to the World Avenue companies and their marketing operations on a continuing basis, including on dates after June, 2009. Regardless, current domain and mapping information is expected to be relevant to prior emails as well. With the recent relocation of at least some of WAUSA's operations to Yacht Haven Grande in St. John's, Virgin Islands, and a series of additional entities and trade names, there is additional data that must be examined in order to identify which emails are attributable to World Avenue. Without the requested domain name and DNS data from Tiggee, BSI's case will be seriously impaired.

For all of the above reasons BSI seeks an order finding DNS Made Easy.com, LLC aka Tiggee in contempt of court for failing to honor the subpoena, compelling Tiggee to make full production, and further imposing sanctions for attorneys fees and costs necessary for the prosecution of this motion

/s/

Stephen H. Ring
STEPHEN H. RING, P.C.
506 Main Street, Suite 215
Gaithersburg, Maryland 20878
MD Bar Id. No. 04731764; USDC, MD: #00405
Telephone: 301-563-9249
Facsimile: 301-563-9639

/s/

Michael S. Rothman
E. Jefferson Street
Suite 201
Rockville, MD 20850
Phone: (301) 251-9660
Fax: (301) 251-9610

Attorneys for Plaintiff

Certificate of Service

I certify that a copy of the foregoing documents was served on the date of ECF filing, via the ECF system, on all counsel of record.

/s/
Stephen H. Ring